Remarks/Arguments

The Examiner is thanked for the careful review of this Application. Claims 1-16, 19, 21, 23-27, 30, 32, and 34-41 are pending after entry of the present Amendment. Claims 17, 18, 20, 22, 28, 29, 31, and 33 have been cancelled. New claims 34-41 have been added. Amendments were made to the specification and claims to correct typographical errors and better define the claimed invention. The new claims and amendments do not introduce new subject matter.

Objections to Drawings:

The Office has objected to Figure 1, as filed on May 14, 2001, as not being designated by a legend. In compliance with the Office's request, the Applicants herein submit Replacement Sheet including Figure 1, as properly designated by the legend "Prior Art." Accordingly, the Applicants respectfully request that objection to the drawings be withdrawn.

Rejections under 35 U.S.C. § 102:

The Office has rejected claims 1, 4, 10-12, 15, 21-23, 26, 32, and 33 under 35 U.S.C. section 102(b) as being anticipated by United States Patent No. 5,684,950 to Dare el al. (hereinafter referred to as Dare). For at least the followings reasons, the Applicants submit that Dare fails to disclose each and every feature of the claimed invention, as defined in amended independent claims 1, 12, and 23, as Dare is directed at single sign-on authentication of an authorized user in a distributed computing environment.

The Applicants respectfully submit that two components, the Kerberos Ticket Granting Ticket (KTGT) and the Kerberos Service Ticket (KST), disclosed in Dare have been interpreted by the Office to be identical to the authenticated token of the claimed invention. Thus, the Applicants cannot identify the specific component interpreted to be the authenticated token of the claimed invention by the Office. Nevertheless, the Applicants respectfully submit that neither the KTGT nor the KST is equivalent to the authenticated token of the claimed invention. In Dare, once the authentication broker has authenticated the user by using the user ID and password, the authentication broker sends the KTGT to the workstation. At this point, to access a Kerberos Ticket Based Server, the KTGT is sent to the broker again subsequent to which the KTGT is exchanged for the KST. Such KST, however, can be used only with one server of the Kerberos servers. To access any of the other Kerberos servers during the same session and while the user is on the same workstation, the user is provided with new and separate KSTs. However, that is contrary to the claimed invention wherein the authenticated token can be used by the user during the same session to access another Kerberos server during the same session. Thus, the KST of Dare is not identical to the authenticated token of the claimed invention.

In the same manner, the KTGT is not identical to the authenticated token of the claimed invention because irrespective of the type of server, the KTGT is sent back to the broker by

Amendments to the Drawings:

The attached sheet of drawings includes changes to FIGURE 1. This sheet replaces the original sheet including FIGURE 1.

Attachment: Replacement Sheet

the workstation, and is exchanged for the KST for accessing a Kerberos server, a pass ticket for accessing a pass-ticket server, and a password to access a password-based server. As the session cannot be accessed using the KTGT, the KTGT fails to perform the same functions as the authenticated token of the claimed invention. Rather, Dare associates the KTGT with the workstation and not the user, as defined in the claimed invention. As such, the Applicants respectfully submit that the claimed invention is novel over the cited prior art.

Rejections under 35 U.S.C. § 103(a):

Claims 2, 13, and 24 have been rejected under 35 U.S.C. 103(a) as being obvious over Dare in view of U.S. Patent No. 6,052,785 to Lin et al. (hereinafter Lin); claims 5-9, 16-20, and 27-31 under 35 U.S.C. 103(a) as being obvious over Dare in view of U.S. Patent No. 6,035,406 to Moussa et al (hereinafter Moussa); and claims 3, 14, and 25 under 35 U.S.C. 103(a) as being obvious over Dare in view of Lin further in view of U.S. Patent No. 6,598,167 to Devine et al. (hereinafter Devine). For at least the reasons provided below, none of the combinations of the cited prior art raises a *prima facie* case of obviousness against the subject matter defined in the claimed invention.

It is respectfully submitted that the teachings of Dare and Lin are not combinable, as modifying Dare using the teachings of Lin renders the single sign-on authentication system of Dare unsuitable for its intended purposes. For instance, in Dare, the authentication broker uses the password and user ID to authenticate the user. Thereafter, the broker sends the KTGT to the workstation, which depending on the type of server the user is seeking access, the KTGT is exchanged with the for example, KST. In Lin, however, the security server attempts to locate the user's stored credentials. If the credentials are not found, the user ID and password are obtained from the user so as to obtain the user's credentials from the repositories. The credentials are thereafter validated and stored in the security server. In achieving such task, Lin has the objective of eliminating the client-remote data repository authentication for all but the first access as well as eliminating repeated requests for authentication from a server once the client has been authenticated. However, Lin's objective is in conflict with Dare's objective on this feature. That is, limiting the number of user's authentication requests during one session (as disclosed in Lin) is in conflict with maintaining constant communication with the server so as to obtain corresponding tickets for the servers being accessed (as disclosed in Dare). If Dare were to be modified so as to limit user authentication to the first access, the user in Dare would not be able to access different types of server within the distributed computer system using the single sing-on authentication. Thus, it is respectfully submitted that Dare and Lin are not combinable.

Furthermore, even if Dare and Lin were combinable (a proposition with which the Applicants disagree), the combination of the two references would not have disclosed, suggested, or taught associating a user with a session using an authenticated token and presenting the authenticated token to access the session from a first terminal and presenting

the same authenticated token to access the session from a second terminal. As described in more detail above in connection with the Applicants' response to the 102(b) rejections, Dare fails to teach, suggest, or disclose an authenticated token, as defined in the claimed invention. In the same manner, Lin fails to teach using an authenticated token to access the session from a first terminal. Rather, Lin teaches storing the credentials for the user and using the credentials to authenticate the user in subsequent accesses. However, the credentials change when the user attempts to access the same remote drive through a different browser (interpreted to be the alleged second terminal of the claimed invention). For instance, in the preferred embodiment, an additional entry is made to the hashtable. Alternatively, the first entry of the user in the hashtable is updated. As such, the user in Lin does not access the session from the first terminal and the second terminal using the authenticated token, as defined in the claimed invention. Additionally, one must note that the second browser may not be a second terminal. Still further, nothing in Devine cures such deficiencies in Dare and Lin. As such, the claimed invention is patentable over Dare in view of Lin as well as Dare in view of Lin further in view of Devine.

Likewise, the teachings of Dare and Moussa are not combinable as Moussa teaches away from Dare. For instance, Moussa teaches using two or more factors simultaneously to authenticate the user so as to make the system more secure. Dare, however, uses the password to authenticate the user. Thus, one of ordinary skill in the art reading the teachings of Moussa would not have been motivated to combine Moussa in which at least two factors are used and Dare in which a password is used together.

Furthermore, Moussa specifically teaches that one of such factors is always the physical token. In fact, Moussa intends to authenticate the user without requiring the user to interact with the physical token. Moussa achieves such task by the user providing a first password along with the physical token including a storage device. The CPU accesses the storage device so as to transform the first password into the second password. Thereafter, the second password is authenticated by the operating system. In Dare, however, the user is authenticated after the password is entered but before the KTGT or KST is sent to the workstation. Thus, the two references authenticate the user at different stages. Yet further, combining Dare and Moussa requires Dare to always use the physical token. However, Dare is silent as to using the physical token or always using the physical token. Additionally, as Dare's system is directed at obtaining passwords, Dare's system would have to be modified significantly to accommodate using the physical token to authenticate the user instead.

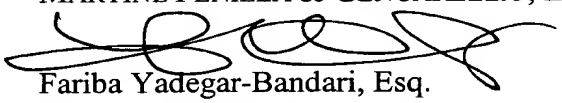
Still further, even if Dare and Moussa were combinable (a preposition with which the Applicant disagrees), the combination of the two references would not have disclosed, suggested, or taught using an authenticated token to associate a user with a session and presenting of the authenticated token by the first terminal, as defined in the claimed invention. Rather, the combination requires to use at least two factors one of which has to be

the physical token. However, having to use two factors simultaneously and using the physical token consistently goes against one of many features of the claimed invention. Specifically, in the claimed invention, the user can access the same session even if the initial token is not present. Making the use of the physical token mandatory is in direct conflict with the claimed invention wherein the user can access the same session even if the initial token is not available. Accordingly, the Applicants kindly request that rejection of the claims under 103(a) be withdrawn.

New independent claim 34 defines a method for accessing a session. Among other features, the method includes authenticating the identity of a user uses the first token of one or more tokens assigned to the user, converting the first token of one or more tokens to an authenticated token, and associating the user with the session using the authenticated token. The authenticated token can be created using each token of the one or more tokens. It is respectfully submitted that the cited prior art fails to disclose, teach, or suggest a method in which each token assigned to the user can be used to associate the user with a session. Furthermore, any of the tokens can be used to allow the user access to the session.

Accordingly, the Applicants respectfully submit that all pending claims are patentable under 35 U.S.C. section 103(a) over any combination of the cited prior art. As such, the Applicants respectfully request examination on the merits of the subject application, and submit that all of the pending claims are in condition for allowance. Accordingly, a notice of allowance is respectfully requested. If the Examiner has any questions concerning the present Amendment, the Examiner is kindly requested to contact the undersigned at (408) 774-6913. If any additional fees are due in connection with filing this Amendment, the Commissioner is also authorized to charge Deposit Account No. 50-0805 (Order No. SUNMP601). A duplicate copy of the transmittal is enclosed for this purpose.

Respectfully submitted,
MARTINE PENILLA & GENCARELLA , LLP



Fariba Yadegar-Bandari, Esq.
Reg. No. 53,805

710 Lakeway Drive, Suite 200
Sunnyvale, CA 94085
Telephone (408) 774-6913
Facsimile (408) 749-6901
Customer No. 32291